NICOLA T. HANNA
United States Attorney
BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division
JULIAN L. ANDRÉ (Cal. Bar No. 251120)
Assistant United States Attorney
Major Frauds Section
1100 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-6683
Facsimile: (213) 894-6269
Email: Julian.L.Andre@usdoj.gov

BRETT A. SAGEL (Cal. Bar. No. 243918)
Assistant United States Attorney
Ronald Reagan Federal Building
411 West Fourth Street, Suite 8000
Santa Ana, California 92701
Telephone: (714) 338-3598
Facsimile: (714) 338-3708
Email: Brett.Sagel@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. MICHAEL JOHN AVENATTI, Defendant.	SA CR No. 19-061-JVS STATUS REPORT REGARDING THE GOVERNMENT'S PRIVILEGE REVIEW

Pursuant to the Court's July 8, 2019, Minute Order (CR 45), plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorneys Julian L. André and Brett A. Sagel, hereby files its Status Report regarding the United States Attorney's Office for the Central District of California's

privilege review of evidence obtained during the course of the investigation of defendant MICHAEL JOHN AVENATTI.

Dated: July 22, 2019

Respectfully submitted,

NICOLA T. HANNA
United States Attorney

BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division

JULIAN L. ANDRÉ
BRETT A. SAGEL
Assistant United States Attorneys

Attorneys for Plaintiff
UNITED STATES OF AMERICA

STATUS REPORT REGARDING PRIVILEGE REVIEW

I. INTRODUCTION

Pursuant to the Court's July 8, 2019, Minute Order (CR 45), the United States Attorney's Office for the Central District of California (the "USAO") submits this status report to address the following topics raised during the July 8, 2019, status conference:

1. The status of the USAO's ongoing privilege review of evidence obtained during the course of its investigation of defendant MICHAEL JOHN AVENATTI ("defendant") and an anticipated timeline for production of documents to the defense.

2. The production of forensic copies of digital devices to defendant and information regarding possible methods for defendant to review the forensic copies that have been produced.

3. Issues relating to the four inaccessible digital devices that law enforcement seized from defendant's residence and from defendant's person during his March 25, 2019, arrest.

This Status Report is based on the information currently available to the USAO's Prosecution Team. To the extent the USAO learns of additional information that may affect the issues addressed herein, the USAO will immediately advise the Court and defendant.

II. THE USAO'S PRIVILEGE REVIEW

A. Evidence To Be Reviewed

As set forth in the parties' July 1, 2019, Joint Report (CR 43), the Internal Revenue Service – Criminal Investigation ("IRS-CI") obtained the following digital devices or forensic copies thereof during the course of its investigation:

1. The computer server belonging to defendant's former law firm, Eagan Avenatti LLP ("EA LLP");

2. Digital devices seized from the residence of EA LLP's former office manager ("EA Employee 1"), which the USAO understands belong to EA LLP or are the personal property of EA Employee 1;

3. Digital devices seized during defendant's arrest on March 25, 2019;

4. Digital devices seized from defendant's residence;

5. Digital devices seized from another law firm with which defendant had a business relationship ("Law Firm 1"); and

6. Digital devices obtained from former employees of defendant's coffee company, Global Baristas U.S. LLC ("GBUS").

The USAO understands that the devices referenced above contain a total of approximately 20 terabytes ("TB") of data. The USAO and IRS-CI obtained warrants to search each of these devices for evidence relating to the investigation of defendant.

IRS-CI also seized approximately 15 to 20 boxes of hard-copy materials during the execution of search warrants at defendant's residence, EA Employee 1's residence, and Law Firm 1's business premises.

B. Status of the Privilege Review

The USAO and IRS-CI are reviewing the contents of the digital devices referenced above, pursuant to the privilege review and other search protocols set forth in the applicable search warrants. The search warrants issued in connection with this investigation require the USAO and IRS-CI to follow specific procedures when reviewing digital devices and other evidence in order to avoid unnecessary

disclosures of attorney-client communications or attorney work product, including the use of a "Privilege Review Team."[1]

1. Review of the EA LLP Server

In order for the Privilege Review Team to efficiently review documents and data stored on the digital devices identified in Section II.A. above, the data on these devices must first be processed, filtered, exported, and loaded into a document review platform. IRS-CI has provided to the Department of Justice's Cybercrime Lab (the "DOJ Lab") the majority of the digital devices obtained by IRS-CI during its investigation, including the EA LLP server and any computers, external hard-drives, and USB drives, so that the DOJ Lab can process and filter the data, and then export the data so it can be loaded into a document review database.

At this time, the Privilege Review Team has prioritized the processing and review of documents and data contained on the forensic image of the EA LLP server. The Privilege Review Team has prioritized the review of the EA LLP server because the EA LLP server likely contains the largest volume of documents and data and because defendant has indicated that documents on the EA LLP server are of particular importance. The Privilege Review Team is also prioritizing the review of any documents or data that appear to relate to the individual client-victims identified in the indictment.

The EA LLP server consists of six separate digital devices, one of which appears to have been EA LLP's email server and another which appears to have been EA LLP's file server. The Privilege Review Team

[1] The Privilege Review Team is being supervised by AUSAs Patrick R. Fitzgerald and Joseph B. Woodring from the USAO's National Security Division.

and DOJ Lab have informed the Prosecution Team that the email server contains approximately 3 million items totaling approximately 3.5 TB, and that the file server contains approximately 19 million items totaling approximately 6.5 TB. The DOJ Lab has processed and filtered all of the data on the EA LLP email and file servers, so that the data can be searched, exported, and then loaded into a document review database. Specifically, the DOJ Lab copied the forensic images to its systems, verified and loaded the forensic image files, filtered out irrelevant system files, expanded any compound files on the EA LLP server (i.e., .zip files), indexed the data so that is could be searched, and then searched the data using initial "scope key words." Undersigned counsel understands that this process took a considerable amount of time due to the large volume of data on the EA LLP server and other technical issues.

The Privilege Review Team and DOJ Lab are in the process of exporting all documents from the email server and file server that were identified as containing any of the initial "scope key words" and loading the documents into a document review database for further review by the Privilege Review Team. The Privilege Review Team and DOJ Lab have recently encountered some technical difficulties during the export process, which should be resolved shortly. Once these technical issues are resolved, the documents and data from the EA LLP server will be loaded into the document review database on a rolling basis.

The USAO currently anticipates that the Privilege Review Team will begin its substantive review of documents and data from the EA

LLP server within one week.[2] The Privilege Review Team will also be reviewing the data from the EA LLP servers to determine whether the initial "scope key words" were effective in identifying documents that fall within the scope of the search warrant. Additionally, the Privilege Review Team is attempting to identify any folders on the EA LLP server that contain information relating to the individual client-victims or other specific categories of documents covered by the search warrants so that the review of these materials can be prioritized.[3]

2. Review of GBUS Digital Devices

As noted above, IRS-CI and the USAO obtained a warrant to search certain digital devices obtained from former GBUS employees. (See CR 1, Ex. 1.) Forensic copies of these devices have already been produced to defendant subject to the Protective Order (CR 36).

To date, the Privilege Review Team and IRS-CI has prioritized the review of one device containing GBUS emails that had been backed up from GBUS's Amazon cloud-based server. The Privilege Review Team has identified potentially privileged documents on this device and is in the process of reviewing such documents pursuant to the search

---

[2] On July 10, 2019, the USAO requested that defense counsel provide the USAO with the names and contact information for any lawyers or law firms with whom defendant or his companies may have had an attorney-client relationship by July 17, 2019. Defense counsel has indicated that he will be responding to this request by the end of this week (i.e., July 26, 2019), at which point any additional names provided by the defense will be added to the USAO's current list of "privilege key words."

[3] The defense is welcome to provide the Privilege Review Team with any information defendant believes may assist the Privilege Review Team in identifying specific client files or any other relevant information on the EA LLP server or other devices. Such information would allow the Privilege Review Team to expedite the review and production of such records to defendant, including the documents and records identified in defendant's portion of the July 1, 2019, joint report (CR 43 at 6).

warrant protocols. The IRS-CI case agents are currently reviewing the non-privileged documents on this device that were released by the Privilege Review Team to determine whether the documents fall within the scope of the search warrant. The USAO has already produced a small number of documents from this review to defendant, and will continue to produce additional documents on a rolling basis going forward.

3. Review of Other Digital Devices and Search Warrant Evidence

The Privilege Review Team and DOJ Lab are currently working to process documents and data from other digital devices obtained during the course of this investigation, using forensic processes similar to those used in connection with the EA LLP server. Documents and data from the other digital devices will be exported and loaded into the document review database on a rolling basis going forward. The DOJ Lab has indicated it should take less time to process the documents and data on the other digital devices than it did to process the data on the EA LLP server.

The Privilege Review Team, however, was already able to identify and locate EA LLP's QuickBooks records on one of the computers seized from EA Employee 1's residence. The Privilege Review Team believes these QuickBooks records contain financial information within the scope of the search warrant and that the privilege review of the records can be completed shortly.

Because smart phones and tablets are typically reviewed using different software programs, such as Cellebrite, the content of any such devices is not being processed by the DOJ Lab or loaded into the document review database. The Privilege Review Team will be

reviewing these devices separately. The Privilege Review Team has already begun the review of EA Employee 1's EA LLP smart phone.

Finally, the Privilege Review Team is working to scan the hard-copy documents seized from defendant's residence, EA Employee 1's residence, and Law Firm 1. Once these documents are scanned, they will be loaded into the documents review database so that the Privilege Review Team can complete its review.

C. Timeline for Completion of the Review and Production of Documents to Defendant

The USAO is working to complete the privilege review as soon as possible. Based on the information currently available, the USAO estimates that the Privilege Review Team will be able to substantially complete the privilege review in the next three to four months. This estimate, however, could change if the volume of documents and data that falls within the scope of the warrants and needs to be reviewed is greater than expected, or if the Privilege Review Team encounters any unexpected technical issues during the review process.

The USAO currently anticipates that it will begin producing non-privileged documents falling with the scope of the search warrants within the next four to six weeks. The USAO expects that the initial production will include the following materials:

- EA LLP's QuickBooks records;
- Emails and other records from the EA LLP server relating to the client-victims identified in the indictment;
- Additional GBUS emails; and
- Data from EA Employee 1's smart phone.

The USAO will then make rolling productions to the defense on a monthly basis going forward. All such documents will be Bates-labeled and produced with database load files, which will allow the defense to more easily search and review the documents.

III. FORENSIC COPIES PRODUCED TO DEFENDANT

On May 15, 2019, defendant requested that the USAO produce forensic copies of any digital devices obtained during the course of its investigation. On June 10, 2019, the Privilege Review Team produced to defendant forensic copies of accessible digital devices seized from defendant's residence, seized during defendant's arrest, and obtained from former GBUS employees. During the July 8, 2019, status conference, defense counsel indicated that he was having difficulties reviewing the forensic copies defendant requested. Accordingly, the Court directed the USAO to include additional information regarding the forensic images that were produced to defendant in the instant report.

IRS-CI has created forensic images of each of the digital devices obtained during the course of this investigation.[4] The purpose of a forensic image is to ensure that the best evidence is collected and that the data on the device can be preserved, authenticated, and verified. The use of a forensic image also allows the parties to preserve metadata and demonstrate that the data on the devices has not been -- and cannot be -- altered.

The production of a forensic image is the standard method for providing a defendant with a complete copy of a hard drive or other

[4] In many instances, such as with the EA LLP server and devices from Law Firm 1, IRS-CI did not maintain a copy of the original devices or never took possession of the original devices.

digital device. Here, the forensic images that were produced to defendant are duplicates of the forensic images that the USAO's Privilege Review Team is using to conduct its own review.

There are a number of commercially available software programs that defendant can use to access, search, and review data on a forensic image, including programs such as Forensic Toolkit (FTK), EnCase, and Nuix. In white-collar prosecutions such as this one, defendants typically retain an eDiscovery vendor or computer forensics expert to assist with the technical aspects of such a review. If defendant is unable to retain such services, the USAO understands that there are some free software programs available online that would allow defense counsel to review the forensic images on his own. For example, there is a free version of FTK Imager available for download from AccessData at https://accessdata.com. The USAO understands that FTK Imager should allow defense counsel to review the folders and most files contained on the forensic images in a format similar to Windows Explorer.

Additionally, based on discussions with an IRS-CI Computer Investigative Specialist, undersigned counsel understands that there is no way for the USAO to ensure that defendant will be able to review the contents of the forensic images in the same manner as he would be able to if defendant were reviewing the original devices. In some limited instances, defendant may be able to use the forensic image of certain devices to create a "virtual machine," which would allow the defense to review the device in a format similar to the original device. Undersigned counsel, however, understands that this is a highly-technical process and that defense counsel may need to obtain technical support to be able to do so.

In sum, the USAO has produced to defendant forensic images of devices in this case in the same manner in which it produces forensic images to defendants in other prosecutions. There is no reason why defendant cannot conduct his own independent review of these forensic images, as numerous other defendants and their counsel do on a regular basis.

IV. INACCESSIBLE DIGITAL DEVICES

As noted in the parties July 1, 2019, joint report (CR 43), IRS-CI is currently in possession of an Apple desktop computer seized from defendant's residence, which is password protected and has not yet been accessed.[5] The United States Attorney's Office for the Southern District of New York is also in possession of an iPhone, an iPad, and an Apple laptop computer, which are password protected and have not yet been accessed. The government will continue its efforts to gain access to these devices pursuant to the warrants. If defendant wishes to immediately obtain forensic copies of these digital devices, defendant can either provide the government with the passwords for these devices or make arrangements to personally unlock the devices.

[5] In defendant's portion of the July 1, 2019, joint report, defendant claimed that the warrants permitting the government to access the inaccessible devices expired. (CR 43 at 14.) This is incorrect. The warrant to search defendant's residence provides the government with at least 180 days to complete the search of any digital devices found in defendant's residence, subject to additional time extensions from the Court. The government may also seek authorization from the Court to retain encrypted devices once the time period to complete the search has concluded.